FortiSandbox VM - Install Guide

Version 2.5.1

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

March 07, 2018
FortiSandbox VM 2.5.1 Install Guide
34-251-457040-20180307

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-01-17	Initial release.
2018-03-07	Updated *Licensing* information.

Introduction

FortiSandbox VM is a 64-bit virtual appliance version of FortiSandbox. It is deployed in a VMware ESXi, Citirx XenServer, or KVM virtual machine environment. Once the virtual appliance is deployed and set up, you can manage FortiSandbox VM via its GUI in a web browser on your management computer.

This document describes how to deploy a FortiSandbox virtual appliance in your virtual server environment. This includes how to configure the virtual hardware settings of the virtual appliance. This guide presumes that the reader has a thorough understanding of virtualization servers.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For that information, see the *FortiSandbox Administration Guide* in the Fortinet Document Library.

FortiSandbox documentation

The following FortiSandbox product documentation is available in the Fortinet Document Library:

- *FortiSandbox Administration Guide*
  This document describes how to set up the FortiSandbox system and use it to manage supported Fortinet units.
- *FortiSandbox QuickStart Guides*
  These documents are included with your FortiSandbox system package. Use these document to install and begin working with the FortiSandbox system and GUI.
- *FortiSandbox Online Help*
  You can get online help from the FortiSandbox GUI. FortiSandbox online help contains detailed procedures for using the GUI to configure and manage devices.
- *FortiSandbox Release Notes*
  This document describes new features and enhancements in the FortiSandbox system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.
- *FortiSandbox VM Install Guide*
  This document, which describes installing FortiSandbox VM in your virtual environment.

Overview

This section provides an overview of FortiSandbox VM. The following topics are included:

Licensing

Fortinet offers the FortiSandbox VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. For information on purchasing a FortiSandbox VM license, contact your Fortinet Authorized Reseller, or visit http://www.fortinet.com/how_to_buy/.

When configuring your FortiSandbox VM, ensure to configure hardware settings as outlined in the following table and consider future expansion. Contact your Fortinet Authorized Reseller for more information.

Technical Specification	Details
Hypervisor Support	VMware ESXi version 5.1, 5.5, or 6.0 and later Citrix XenServer 6.5 and later Kernel Virtual Machine (KVM)
HA Support	FortiSandbox 2.1.0 and later
Virtual CPUs (min / max)	4 / Unlimited*
Virtual Network Interfaces	6
Virtual Memory (min / max)	8GB / Unlimited**
Virtual Storage (min / max)	200GB / 16TB***

* Fortinet recommends that the number of virtual CPUs is four plus the number of Windows VMs.

** Fortinet recommends that the size of virtual memory is 8GB plus 3 GB for every Windows VM clone.

*** Fortinet recommends that the size of virtual storage is 1TB for production environment.

For more information, see the FortiSandbox product data sheet available on the Fortinet web site, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf.

After placing an order for FortiSandbox VM, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiSandbox VM with Customer Service & Support at https://support.fortinet.com.

Upon registration, you can download the license file. You will need this file to activate your FortiSandbox VM. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded and validated, the CLI and GUI will be fully functional.

FSA-VM and FSA-VM00

The VM model available to order is FSA-VM00, which replaces previous FSA-VM model.

For previous FSA-VM models, its base license contains four Windows license keys to activate four different Windows VM in the base VM package. Users can purchase 50 more Windows license keys to allow the unit to run at most 54 Windows clones.

The serial number of FSA-VM model starts with *FSA-VM*. Starting from Q3, 2017, the licenses for this model are no longer available for purchase. However, user can still upgrade the existing installations with new firmware releases.

For the new FSA-VM00 models, the base license does not contain a Windows license key. Users can purchase the needed Windows license keys to activate enabled Windows VMs. For example, if the user only wants to use Window 8 VMs, the user can purchase Windows 8 license keys. The maximum allowed Windows clones for FSA-VM00 model is eight. The serial number for FSA-VM00 models starts with *FSAVM0*.

System requirements

Prior to deploying the FortiSandbox VM virtual appliance, VMware vSphere Hypervisor (ESXi version 5.1, 5.5, 5.0, and later), Citrix XenServer (6.5 and later), or KVM must be installed and configured. The installation instructions for FortiSandbox VM assume you are familiar with your VM server and terminology.

Upgrade to the latest, stable update and patch release for your virtual environment.

FortiSandbox VM has specific CPU requirements: Intel Virtualization Technology (VT-x/EPT) or AMD Virtualization (AMD-V/RVI).
Enter the BIOS to enable Virtualization Technology and 64-bit support.
Detailed information can be found at https://communities.vmware.com/docs/DOC-8970.

Ensure the following prerequisites are met before installing FortiSandbox VM:

VMware:

- The VMware vSphere ESXi Hypervisor software must be installed and configured.
  - ESXi version 5.1: Hardware version 9
  - ESXi version 5.5: Hardware version 9 or 10
  - ESXi version 6.0: Hardware version 9, 10, or 11
- The VMware vSphere client is installed on the management computer.

Citrix:

- XenServer 6.5 or later must be installed and configured.
- The Citrix XenCenter client is installed on the management computer.

KVM:

- A compatible Linux distribution, such as Ubuntu 16.04 with Kernel 4.6.7 and later and the qemu-kvm 2.5 and later packages, or CentOS 7.2 with Kernel 4.1.12 and later and the qemu-kvm 2.3 and later packages.
- virt-manager is installed on the management computer.

Register with Customer Service & Support

To obtain the FortiSandbox VM license file you must first register your FortiSandbox VM with Fortinet Customer Service & Support.

To register your FortiSandbox VM:

1. Log in to the Fortinet Customer Service & Support portal using an existing support account or select *Create an Account* to create a new account.
2. In the toolbar select *Asset* > *Register/Renew*. The *Registration Wizard* opens.
3. Enter the registration code from the FortiSandbox VM License Certificate that was emailed to you, then select *Next*. The *Registration Info* page is displayed.
4. Enter your support contract number, product description, Fortinet Partner, and IP address in the requisite fields, then select *Next*.

As a part of the license validation process FortiSandbox VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiSandbox VM's IP address has been changed, the FortiSandbox VM must be rebooted in order for the system to validate the change and operate with a valid license.

The Customer Service & Support portal currently does not support IPv6 for FortiSandbox VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

5. On the *Fortinet Product Registration Agreement* page, select the checkbox to indicate that you have read, understood, and accepted the service contract, then select *Next* to continue to the *Verification* page.
6. The verification page displays the product entitlement. Select the checkbox to indicate that you accept the terms then select *Confirm* to submit the request.
7. From the *Registration Completed* page you can download the FortiSandbox VM license file, select *Register More* to register another FortiSandbox VM, or select *Finish* to complete the registration process.

   Select *License File Download* to save the license file (`.lic`) to your management computer. See Upload the license file on page 38 for instructions on uploading the license file to your FortiSandbox VM via the GUI.

To edit the FortiSandbox VM IP address:

1. In the toolbar select *Asset* > *Manage/View Products* to open the *View Products* page.
2. Select the FortiSandbox VM serial number to open the *Product Details* page.
3. Select *Edit* to change the description, partner information, and IP address of your FortiSandbox VM from the *Edit Product Info* page.
4. Enter the new IP address then select *Save*.

You can change the IP address five (5) times on a regular FortiSandbox VM license. There is no restriction on a full evaluation license.

5. Select *License File Download* to save the license file (`.lic`) to your management computer. See Upload the license file on page 38 for instructions on uploading the license file to your FortiSandbox VM via the GUI.

Download the deployment package

FortiSandbox VM deployment packages are included with firmware images on the Customer Service & Support site.

- FSA_VM-v2xx-build0xxx-FORTINET.out: Download this firmware image to upgrade your existing FortiSandbox VM installation.
- FSA_VM-v2xx-build0xxx-FORTINET.out.ovf.zip: Download this package for a new FortiSandbox VM installation on ESXi server or Citrix XENserver.
- FSA_VM-v2xx-build0xxx-FORTINET.out.kvm.zip: Download this package for a new FortiSandbox VM installation on KVM.

For more information see the FortiSandbox VM datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortisandbox/advanced-threat-protection-appliances.html.

Firmware images FTP directories are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model.

You can download the *FortiSandbox Release Notes* and FortiSandbox and Fortinet core MIB files from this directory.

Download the `.out` file to upgrade your existing FortiSandbox VM installation.

To download the firmware package:

1. Log in to the Fortinet Customer Service & Support portal then, from the toolbar, select *Download* > *Firmware Images*. The *Firmware Images* page opens.
2. Select *FortiSandbox* from the *Select Product* drop-down list, then select *Download*.
3. Browse to the appropriate directory for the version that you would like to download.
4. Download the appropriate firmware image and release notes to your management computer.
5. Extract the contents of the package to a new folder on you management computer.

Deployment package contents

The `.out.ovf.zip` file contains:

- `fsa.vmdk`: The FortiSandbox VM system hard disk in Virtual Machine Disk (VMDK) format.
- `FortiSandbox-VM.ovf`: The VMware virtual hardware configuration file.
- `DATADRIVE.vmdk`: The FortiSandbox VM log disk in VMDK format

The `out.kvm.zip` file contains:

- `image.out.qcow2`: The FortiSandbox VM firmware.
- `datadrive.qcow2`: The data drive.
- `fas-kvm.sh`: The installation script for easy installation.

Deploying the appliance

Prior to deploying the FortiSandbox VM, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiSandbox VM presume that you are familiar with the management software and terminology of your VM platform.

For assistance in deploying FortiSandbox VM, refer to the deployment examples in this guide. You may also need to refer to the documentation provided with your VM server. The deployment chapters are presented as examples because, for any particular VM server, there are multiple ways of creating a virtual machine - command line tools, APIs, alternative graphical user interface tools.

Before you start your FortiSandbox VM appliance for the first time, you might need to adjust virtual disk sizes, networking settings, and CPU configuration. The first time you start FortiSandbox VM, you will have access only through the console window of your VM server environment. After you configure one network interface with an IP address and administrative access, you can access the FortiSandbox VM GUI (see GUI access on page 36).

Citrix XenServer deployment example

Once you have downloaded the `FSA_VM-v2xx-build0xxx-FORTINET.out.ovf.zip` file and extracted the files, you can create the virtual machine in your Citrix Xen environment.

The following topics are included in this section:

- Create the virtual machine
- Start the virtual machine

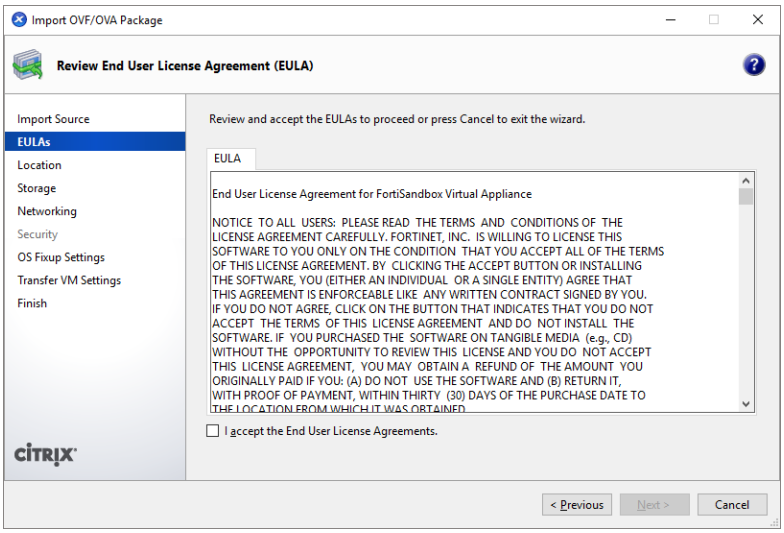
Create the virtual machine

To create the virtual machine:

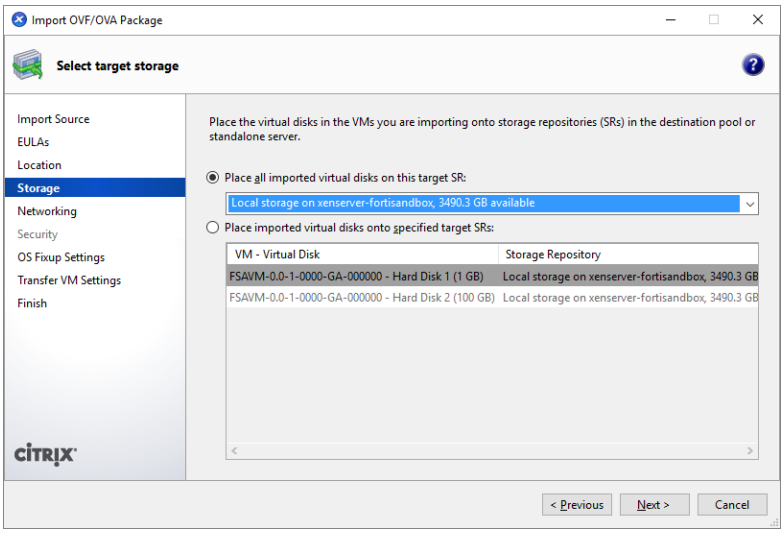
1. Launch XenCenter on your management computer.

   The management computer can be any computer that can run Citrix XenCenter.
2. Select *ADD a server*, then enter the Citrix XenServer IP address and the root logon credentials required to manage that server.

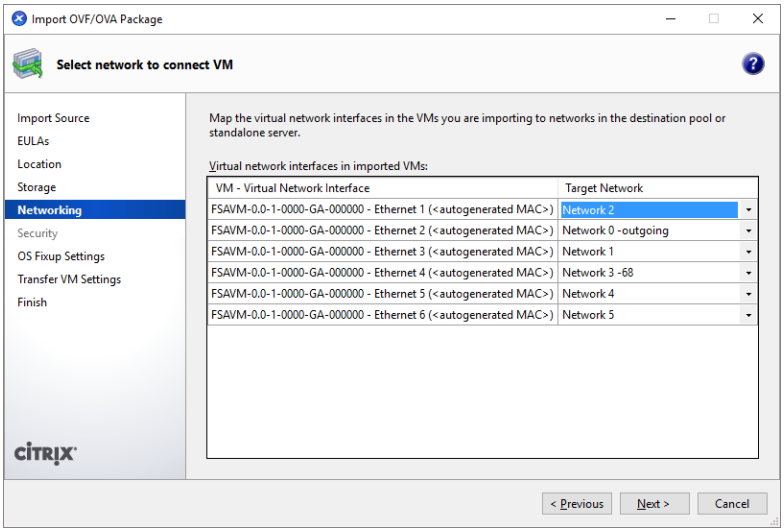
   Your Citrix XenServer is added to the list in the left pane, and the *Virtual Machine Manager* home page opens.
3. Select *File* > *Import*.
4. Select *Browse*, locate the `FortiSandbox-VM.ovf` file, select *Open*, then click *Next*.
5. Accept the End User License Agreement, then click *Next*.



6. Choose the pool or standalone server that will host the VM, then click *Next*.
7. Select the default storage location for the FortiSandbox VM disk drives - *Place all imported virtual disks on this target SR* - then click *Next*.



8. Configure the virtual network interfaces:
   - The *Target Network* for Ethernet 1 should be in the management network segment.

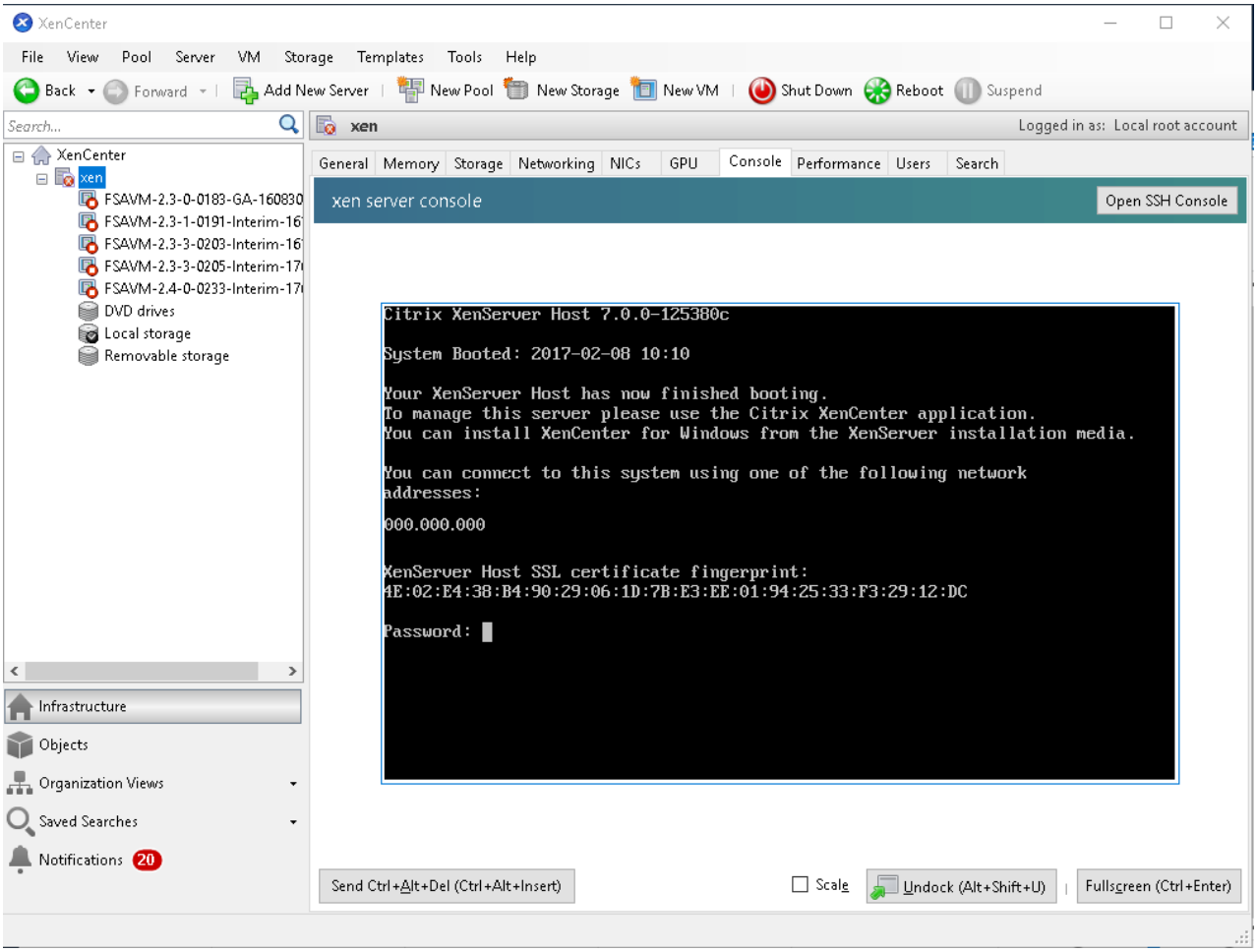


9. Click *Next* to continue.
10. Ensure that *Don't use Operating System Fixup* is selected, then click *Next*.
11. Configure the networking options for the transfer VM, which runs on the network that your Citrix XenServer is running:
    - Select a network from the list of network interfaces that are available in the destination pool or standalone server.
    - To use DHCP to automatically specify network settings, select *Automatically obtain network settings using DHCP*.
    - To configure the network settings manually, click *Use these network settings* and then enter the IP address, subnet mask, and gateway in their requisite fields.

    Click *Next* to continue.
12. Review the VM settings, then click *Finish* to import the VM. The FortiSandbox VM will take approximately 15 minutes to initialize.

    When the VM import is complete, the XenServer left pane will include the FortiSandbox VM in the list of deployed VMs for your Citrix XenServer.

13. Ensure the imported FSAVM instance is in the shutdown state.
14. In the *XenCenter* left pane, select the XenServer labeled as "*xen*". Then, enter the following commands in the `dom0` console tab:



Get the UUID of the FSAVM instance, xe vm-list name-label=<FSAVM_name>

[root@xen ~]# xe vm-list name-label=FSAVM-2.4-0-0233-Interim-170207

uuid (RO) : 1d4be338-e137-e19d-ea0e-2ac5bb2a7a7e

name-label (RW): FSAVM-2.4-0-0233-Interim-170207

power-state (RO): running

Check FSAVM instance platform params,

[root@xen ~]# xe vm-param-get uuid=1d4be338-e137-e19d-ea0e-2ac5bb2a7a7e param-name=platform

pae: true; stdvga: 0; acpi: true; apic: true; nx: true

Enable the FSAVM instance as a nested hypervisor, xe vm-param-set uuid=<UUID> platform:exp-nested-hvm=true

[root@xen ~]# xe vm-param-set uuid=1d4be338-e137-e19d-ea0e-2ac5bb2a7a7e platform:exp-nested-hvm=true

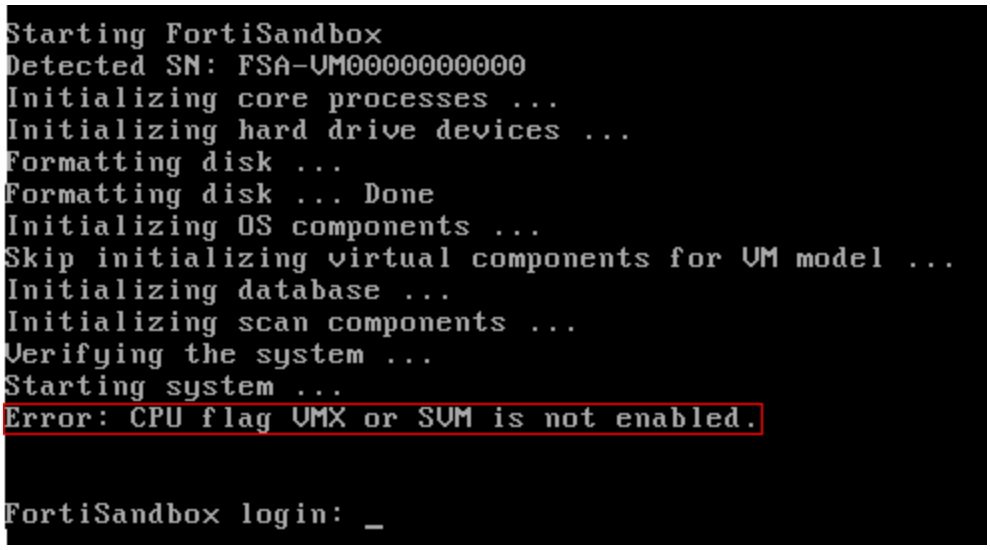
Check FSAVM instance platform params

[root@xen ~]# xe vm-param-get uuid=1d4be338-e137-e19d-ea0e-2ac5bb2a7a7e param-name=platform

exp-nested-hvm: true; pae: true; stdvga: 0; acpi: true; apic: true; nx: true

[root@xen ~]#

If you do not correctly enter the commands, the *CPU flag VMX or SVM is not enabled* error message will appear when booting up the FSAVM.



15. Start the FSAVM instance and the ensure the FSAVM Hypervisor is up and running.

Assigning 4 vCPUs to FortiSandbox VM on XenServer 7.0

If you need to assign more than 4 vCPUs to FortiSandbox on XENserver 7.0, and you have trouble booting up and the following error message appears: `xen_netfront: can't alloc rx grant refs` in the console, use the following instructions to fix the issue.

1. Run XenCenter, and connect to your XENserver.
2. Click *Tools*, and click *Install Updates*.
3. Follow the wizard and apply *Hotfix XS70E034* to your XENserver.
4. Execute the following command in DOM0 console and reboot the XENserver.
   `/opt/xensource/libexec/xen-cmdline --set-xen gnttab_max_frames=128`
5. FSAVM00_b0252 starts with 8 vCPUs as expected.

Start the virtual machine

You can now proceed to start on your FortiSandbox VM.

- In the XenCenter left pane, right-click on the name of the FortiSandbox VM and select *Start*.
- Select the name of the FortiSandbox VM from the left pane, then select *Start* in the toolbar.

KVM deployment example

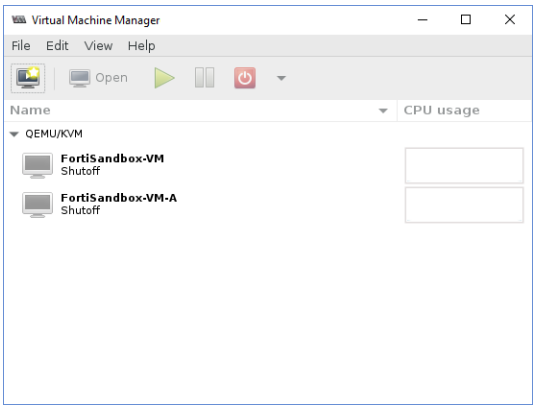
Once you have downloaded the `FSA_VM-v2xx-build0xxx-FORTINET.out.kvm.zip` file and extracted files, you can create the virtual machine in your KVM environment.

Create the virtual machine

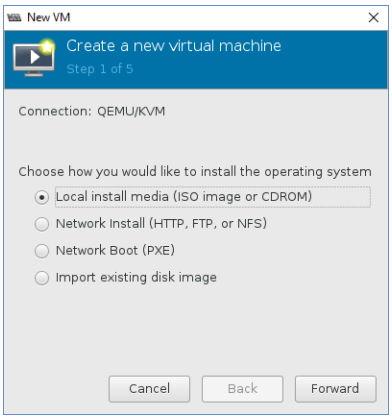
To create the virtual machine:

The easy way to create the virtual machine is to execute the `fas-kvm.sh` script in shell. You can also install it manually. To do that:

1. Launch Virtual Machine Manager (virt-manager) on you KVM host server. The *Virtual Machine Manager* home page opens.



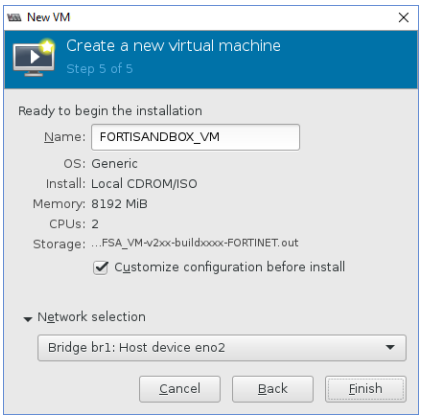
2. Select *Create a new virtual machine* from the toolbar.



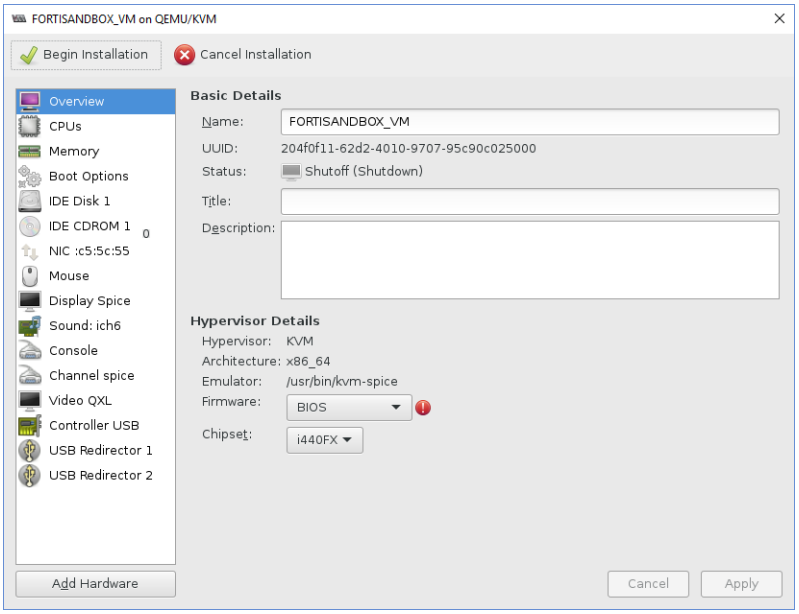
3. Select *Import existing disk image*, then click *Forward*.
4. Enter the full path to extract the `image.out.qcow2` file or click *Browse*.If you copied the file to `/var/lib/libvirt/images`, it will be shown on the right. If you saved it elsewhere on the server, select *Browse Local* to find it.
5. Click *Forward*.
6. Specify the amount of memory and the number of CPUs to allocated to this VM, then click *Forward*.

   A minimum of 8GB of memory and two CPUs are required for the VM. Fortinet recommends that the number of CPU cores be four more than the number of Windows VMs, and 3GB of RAM per Windows VM.

   a. Click *Forward* and set the name of your VM.
   b. Select *Customize Configuration before install*.
   c. Select the correct interface for the *Network Selection* field.

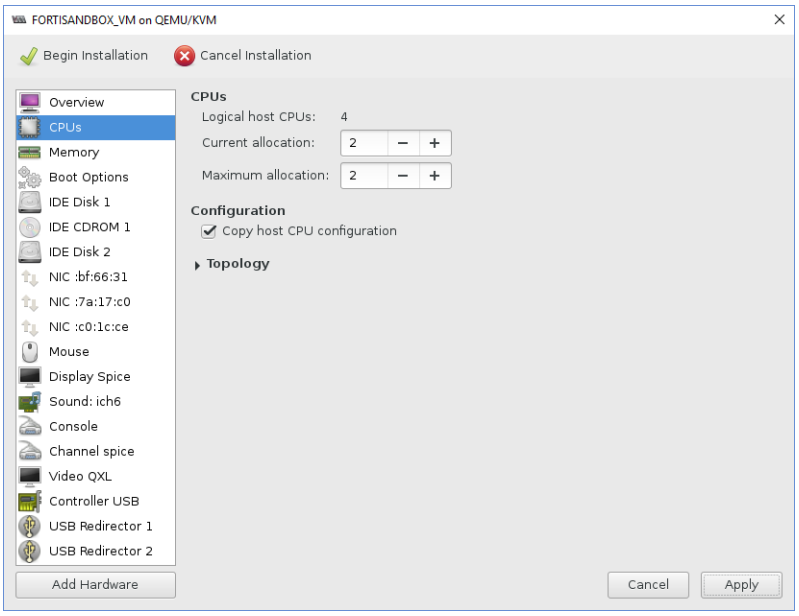


7. Click *Finish*. The Virtual Machine Manager opens.

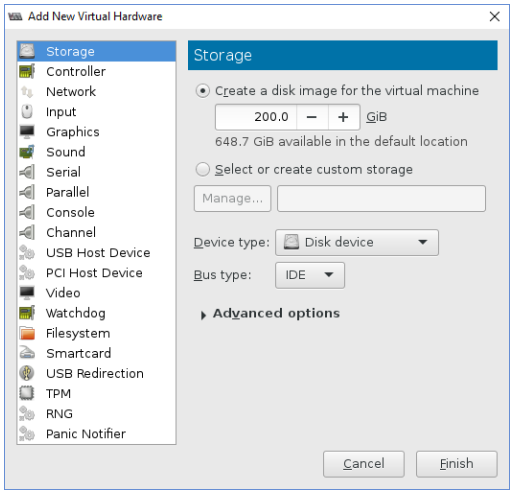


Before powering on your FortiSandbox VM you must configure the CPUs to copy the host configuration, and add a local hard drive of at least 200GB and at least two more network interfaces.

8. Select *CPUs from the list > Copy host CPU Configuration > Apply*.



9. Add a second hard drive:
   a. Click *Add Hardware* > *Storage*.

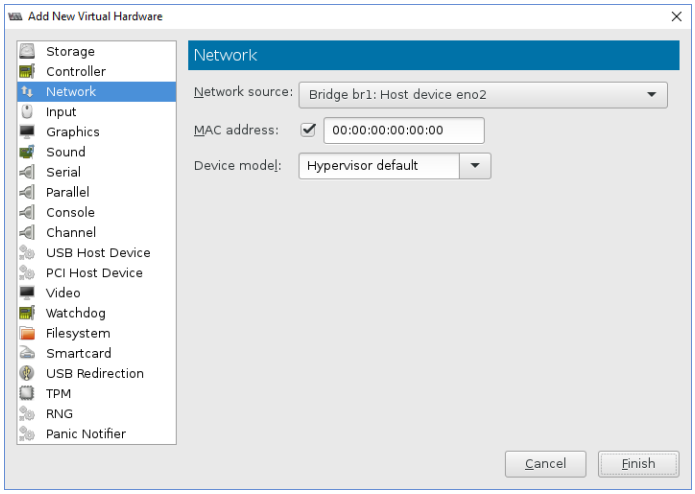


   b. Enter *200* or a larger number in the disk size field, then click *Finish*. Fortinet recommends making the virtual disk 1TB or larger.

      The disk is created and added to the hardware list as *IDE Disk 2*.

10. Add more network interfaces:

a. Click *Add Hardware* > *Network*.

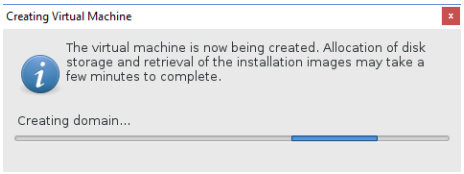


b. Edit the settings as required, then click *Finish* to create the interface.

c. Repeat these steps to create a third interface.

FortiSandbox VM supports up to six network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.

11. Click *Begin Installation* to create the VM.



The FortiSandbox VM is created and started. See Initial Configuration on page 35 for information on configuring your FortiSandbox VM.

VMware deployment example

The FortiSandbox VM can be deployed and configured using VMware vSphere Hypervisor™ (ESX/ESXi) and VMware vSphere Client™, or with VMware Player™.

VMware vSphere

Once you have downloaded the `FSA_VM-v210-build0xxx-FORTINET.out.ovf.zip` file and extracted the package contents to a folder on your management computer, you can deploy the OVF package to your VMware environment.

Prior to deploying the FortiSandbox VM, ensure that the following are configured and functioning properly:

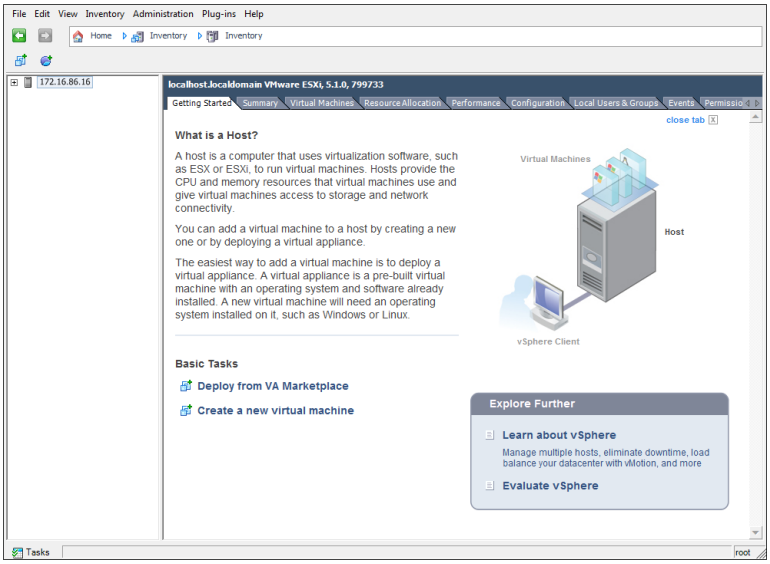
- VMware vSphere Hypervisor™ (ESX/ESXi) software must be installed on a server prior to installing FortiSandbox VM. Go to http://www.vmware.com/products/vsphere-hypervisor/index.html for installation details.
- VMware vSphere Client™ must be installed on the computer that you will be using for managing the FortiSandbox VM.

The following topics are included in this section:

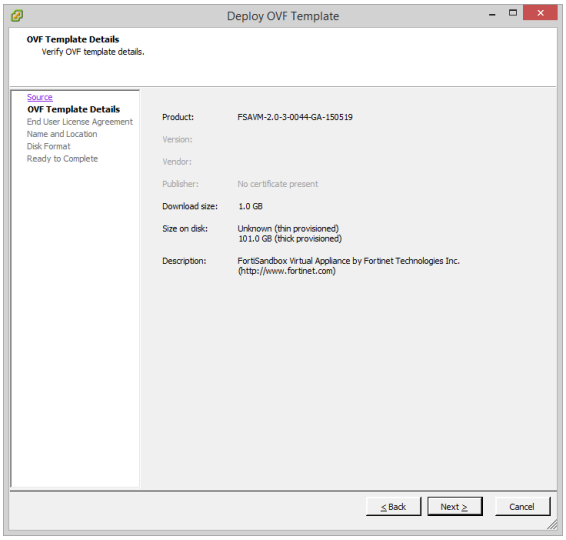
Deploy the OVF file

To deploy the OVF file template:

1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password, then select *Login*. The vSphere client home page opens.

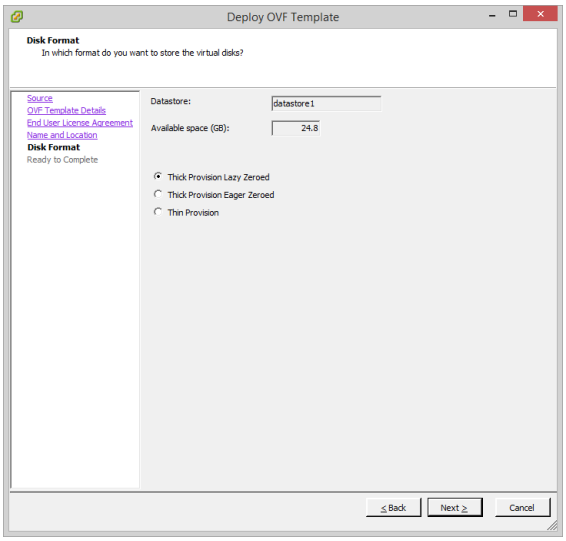


2. Select *File* > *Deploy OVF Template* to launch the OVF Template wizard. The OVF Template *Source* page opens.
3. Select *Browse*, locate the OVF file on your computer, then select *Next* to continue. The OVF Template *Details* page opens.



4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Select *Next* to continue. The OVF Template *End User License Agreement* page opens.
5. Read the end user license agreement, then select *Accept* then *Next* to continue. The OVF Template *Name and Location* page opens.

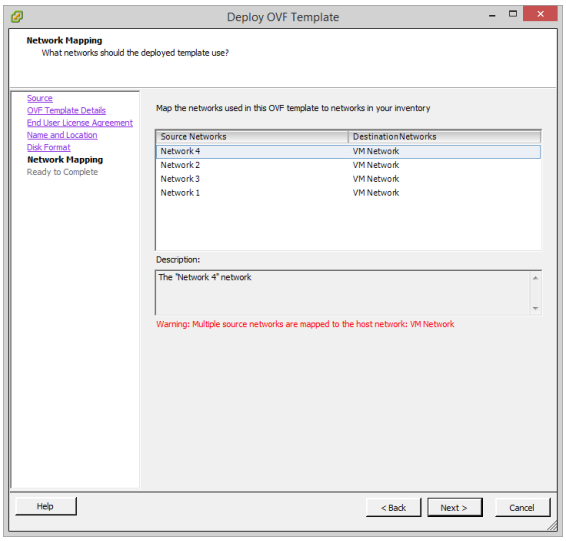
6. Enter a name for this OVF template. The name can contain up to 80 characters and it must be unique within the inventory folder. Select *Next* to continue. The OVF Template *Disk Format* page opens.



7. Select one of the following:
   - *Thick Provision Lazy Zeroed*: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
   - *Thick Provision Eager Zeroed*: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
   - *Thin Provision*: Allocates the disk space only when a write occurs to a block, but the total volume size is reported by the Virtual Machine File System (VMFS) to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains in the volume regardless of if you have deleted data, etc.

If you know your environment will expand in the future, it is recommended to add hard disks larger than the 200GB FortiSandbox VM base license requirement and utilize Thin Provision when setting the OVF Template disk format. This will allow your environment to be expanded as required while not taking up more space in the SAN than is needed.

8. Select *Next* to continue. The OVF Template *Network Mapping* page opens.



9. Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the FortiSandbox VM. You must set the destination network for this entry to access the device console. Select *Next* to continue. The OVF Template *Ready to Complete* page opens.
10. Review the template configuration.

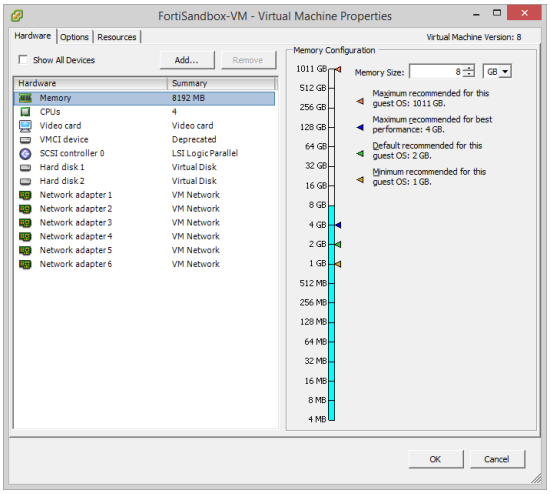
    Ensure that *Power on after deployment* is not enabled. You need to configure the FortiSandbox VM hardware settings prior to powering on the VM.
11. Select *Finish* to deploy the OVF template. You will receive a *Deployment Completed Successfully* dialog box once the FortiSandbox VM OVF template wizard has finished.

Configure hardware settings

Before powering on your FortiSandbox VM you must configure the virtual memory, virtual CPU, and virtual disk.

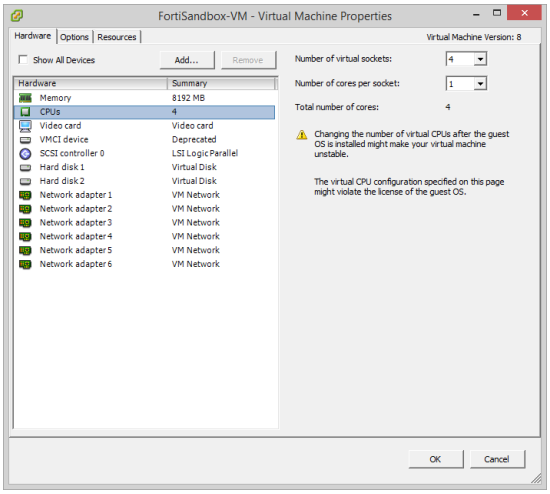
To configure the VM:

1. In the vSphere Client, right-click on the FortiSandbox VM in the left pane and select Edit Settings to open the *Virtual Machine Properties* window.
2. Select *Memory* from the *Hardware* list, then adjust the *Memory Size* as required. 3GB of RAM per Windows VM is recommended.

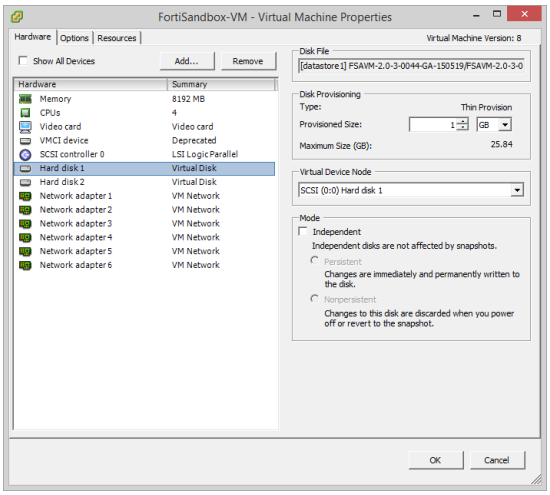


3. Select *CPUs* from the *Hardware* list, then adjust the *Number of virtual sockets* and *Number of cores per socket* as required.

If you need to change the vCPUs after the initial boot, power off FortiSandbox VM. Fortinet recommends that the number of vCPUs be four more than the number of Windows VMs.



4. Select *Hard disk 2*, the data disk, from the *Hardware* list, and configure it as required. Fortinet recommends making the virtual disk 1TB or larger. *Hard disk 1* should not be edited.



5. Select a network adapter from the *Hardware* list, then adjust the virtual network mapping as required by your network configuration. To use sniffer mode promiscuous mode must be enable on a port, see Sniffer mode.

By default, six bridging virtual network adapters are created and automatically mapped to a port group on a virtual switch (vSwitch) in the virtual server. Each of the network adapters can be used by one of the six network interfaces in the FortiSandbox VM. The default mappings are appropriate when each of the host's guest virtual machines have their own IP address on your network.

6. Select *OK* to apply your changes.

Sniffer mode

To use sniffer mode, promiscuous mode must be enable on a port of your VMware server.

To enable promiscuous mode:

1. In the vSphere client, select your VMware server in the left pane, then select the *Configuration* tab in the right pane.
2. In the *Hardware* list, select *Networking*.
3. Select *Properties* for the switch, such as *vSwitch0*. The properties window opens.
4. In the *Ports* tab, select *vSwitch*, then select *Edit*. to open the switch properties window.
5. Select the *Security* tab.
6. In the *Promiscuous Mode* drop-down list select *Accept*, then select *OK*, and then *Close*.
7. Repeat the process for any further switches.

Power on the virtual machine

You can now proceed to power on your FortiSandbox VM.

- Select the FortiSandbox VM in the left pane and select *Power on the virtual machine* in the *Getting Started* tab.
- Select the VM in the left pane, then select *Power On* in the toolbar.
- Right-click the VM in the left pane, then select *Power* > *Power On* from the right-click menu.

Initial Configuration

Before you can connect to the FortiSandbox VM you must configure basic configuration via the CLI console. Once configured, you can connect to the FortiSandbox VM GUI and upload the FortiSandbox VM license file that you downloaded from the Customer Service & Support portal.

The following topics are included in this section:

- GUI access
- Upload the license file
- Install the Windows VM package
- Configure your FortiSandbox VM

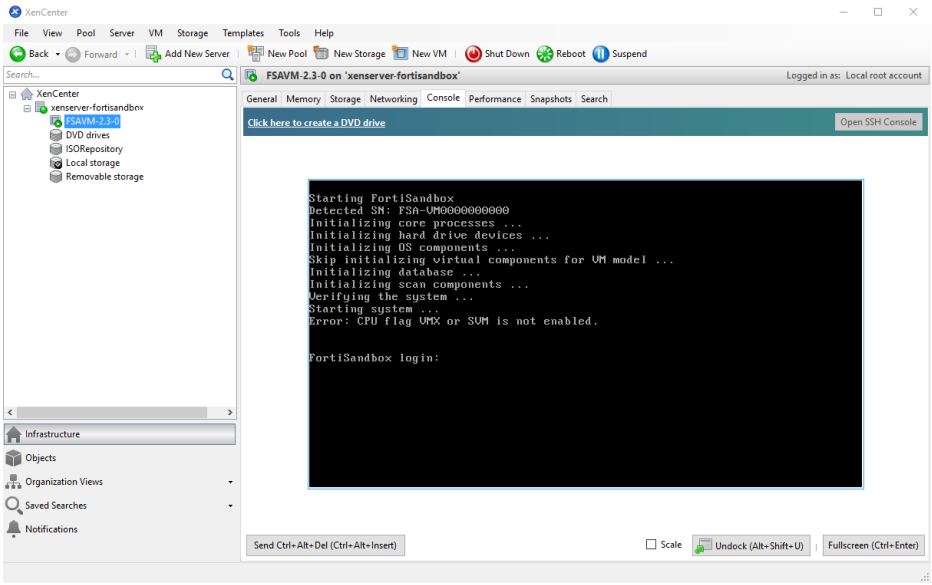
GUI access

Enable GUI access

To enable GUI access to the FortiSandbox VM you must configure the port1 IP address and network mask of the FortiSandbox VM.

To configure the port1 IP address and netmask:

1. In your hypervisor manager, start the FortiSandbox VM and access the console window. You might need to press *Enter* to see the login prompt.



2. At the FortiSandbox VM login prompt, enter the username *admin*, then press *Enter*. By default, there is no password.
3. Using CLI commands, configure the port1 IP address and netmask with the following command:

   set port1-ip <ip address>/<netmask>
4. Configure the static route for the default gateway with the following command:

   set default-gw <default gateway>

The Customer Service & Support portal does not currently support IPv6 for FortiSandbox VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

Connect to the GUI

Once you have configured the port1 IP address and network mask, launch a web browser and enter the IP address you configured for the port management interface. By default the GUI is accessible via HTTPS. At the login page, enter the

user name `admin` and no password, then select *Login*.

Upload the license file

Before using the FortiSandbox VM you must enter the license file that you downloaded from the Customer Service & Support portal upon registration.

To upload the license file:

1. Log in to the FortiSandbox VM GUI and find the *System Information* widget on the dashboard.
2. In the *VM License* field, select `Upload License`. The *VM License Upload* page opens.
3. Select *Browse*, locate the VM license file (`.lic`) on your computer, then select *OK* to upload the license file.
   A reboot message will be shown, then the FortiSandbox VM system will reboot and load the license file.
4. Refresh your browser and log back in to the FortiSandbox VM(username *admin*, no password).
   The VM registration status appears as valid in the *System Information* widget once the license has been validated.

As a part of the license validation process FortiSandbox VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiSandbox's IP address has been changed, the FortiSandbox VM must be rebooted in order for the system to validate the change and operate with a valid license.

If the IP address in the license file and the IP address configured in the FortiSandbox VM do not match, you will receive an error message when you log back into the VM.
If this occurs, you will need to change the IP address in the Customer Service & Support portal to match the management IP and re-download the license file.
To change the management IP address, see To edit the FortiSandbox VM IP address: on page 10

Install the Windows VM package

To complete the installation, the Microsoft Windows VM package must be downloaded and installed either manually or automatically, and then activated.

To manually download and install the package:

1. **For FSA-VM model:**

   The base package can be downloaded from ftp://fsavm.fortinet.net/general/image/2.0.0/2015022118_vm.pkg.7z

   The following Windows VM are contained in the package:

   - WINXPVM (Windows XP with Microsoft Office installed, 32 bit)
   - WINXPVM1 (Windows XP, 32 bit)
   - WIN7X86VM (Windows 7 with Microsoft Office installed, 32 bit)
   - WIN7X64VM (Windows 7, 64 bit)

   The base license file contains Windows license keys and Microsoft Office key to activate them. Users can also purchase, download and install extra Android, Windows 8.1 and Windows 10 image packages. These packages can be downloaded from:

   Android:

   Download the package from ftp://fsavm.fortinet.net/images/v2.00/AndroidVM.pkg.7z

   Windows 8.1:

   Download the package from ftp://fsavm.fortinet.net/images/v2.00/WIN81VM.pkg.7z

   Windows 10:

   Download the package from ftp://fsavm.fortinet.net/images/v2.00/WIN10VM.pkg.7z

   For FSA-VM00 model:

   The base package is optional but recommended to install. The user can choose to automatically install the necessary VM. See To automatically download and install the package: on page 40 for more detailed information.

   The default base package can be downloaded from ftp://fsavm.fortinet.net/images/v2.00/VM00_base.pkg

   The following VMs are contained in the package:

   - WINXPVM (Windows XP with Microsoft Office installed, 32 bit)
   - WIN7X86VMO16 (Windows 7 with Microsoft Office installed, 32 bit)
   - WIN81X64VM (Windows 8.1, 64 bit)
   - WIN10X64VM (Windows 10, 64 bit)

   MD5 File:

   Download the md5 value of images from ftp://fsavm.fortinet.net/images/v2.00/md5.txt

   Downloading the Windows VM package with a web browser is not recommended due to the size of the file. An FTP client that supports resume download is recommended.

2. Put the package on a host that supports file copy with the SCP or FTP command. The FortiSandbox must be able to access the SCP or FTP server.
3. In a console window, enter the following command string to download and install the package:

   fw-upgrade -v --s<SCP/FTP server IP address> -u<user name> -p<password> -t<ftp|scp> -f<file path>

Windows Sandbox VMs must be activated against the Microsoft activation server. This is done automatically after a system reboot. To make sure the activation is successful, port3 of the system must be able to access Internet, and the DNS server should be available to resolve the Microsoft activation servers.

To automatically download and install the package:

FortiSandbox can automatically check for and download new Microsoft Windows VM packages. Login to the unit, go to *Virtual Machine* > *VM Images* page, download and install the *Windows VM* image needed. The system must be able to access https://fsavm.fortinet.net. Detailed information can be found in the *FortiSandbox Administration Guide*, under the *Virtual Machine* > *VM Images* section.

Install Windows license key file for newly installed Windows VM if needed

Windows license keys might be needed to activate newly installed Windows VMs. The user needs to purchase them from Fortinet and install the license file. For example, the base license for FSA-VM00 model does not contain any Windows license key. Windows license keys are stackable, which means newly ordered Windows keys will be appended to existing ones and the new license file will contain all ordered keys.

For FSA-VM00 models, users can just purchase Windows license keys for enabled Windows VM only. For example, if user only enables WIN7X86VMO16 VM, only Windows 7 license keys and Microsoft Office keys are needed.

1. Download the Key license file from the Fortinet Customer Service & Support portal.
2. Log in to the FortiSandbox VM GUI and find the *System Information* widget on the dashboard.
3. In the *VM License* field, select *Upload License*. The *VM License Upload* pane opens.
4. Browse to the license file on the management computer then click *Submit*. The FortiSandbox VM will reboot. The Windows VM or Microsoft Office on it is automatically activated against the Microsoft activation server when the system is rebooted.

For the VM unit, the number of simultaneously scanned Microsoft Office files is limited by the number of installed Microsoft Office license keys. Users can purchase extra Microsoft Office license keys to improve Office file scan capacity.

To ensure that the Windows VM and Microsoft Office activation is successful, port3 must be able to access the Internet, and the DNS servers must be able to resolve the Microsoft activation servers.

Configure your FortiSandbox VM

Once the FortiSandbox VM license has been validated, you can configure your device. For more information on configuring your FortiSandbox VM, see the *FortiSandbox Administration Guide* available in the Fortinet Document Library.

Glossary

A

AAA
Authentication, Authorization, and Accounting

AD
Active Directory

ADOM
Administrative Domain

AES
Advanced Encryption Standard

AMI
Amazon Machine Image

AP
Access Point

API
Application Programming Interface

APN
Access Point Name

APT
Advanced Persistent Threat

ATP
Advanced Threat Protection

AV
Antivirus

AVP
Attribute Value Pairs

AWS
Amazon Web Service

B

BGP
Border Gateway Protocol

C

C&C
Command and Control

CA
Certificate Authority

CASI
Cloud Access Security Inspection

CBC
Cipher Block Chaining

CHAP
Challenge-Handshake Authentication Protocol

CIDR
Classless Inter-Domain Routing

CLI
Command Line Interface

CN
Common Name

CoA
Change of Authorization

CPU
Central Processing Unit

CRL
Certificate Revocation List

CSR
Certificate Signing Request

CSV
Comma Separated Value

CVE
Common Vulnerabilities and Exposures

D

DC
Domain Controller, Direct Current

DES
Data Encryption Standard

DH
Diffie-Hellman

DHCP
Dynamic Host Configuration Protocol

DLL
Dynamic-Link Library

DLP
Data Loss Prevention

DN
Distinguished Name

DNAT
Destination Network Address Translation

DNS
Domain Name System

DSCP
Differentiated Services Code Point

DSRI
Disable Server Response Inspection

DTLS
Datagram Transport Layer Security

E

EA
E-mail Address

EAPOL
Extensible Authentication Protocol over LAN (Local Area Network)

EC
Endpoint Control

EC2
Elastic Compute Cloud

EGP
Exterior Gateway Protocol

EMS
Enterprise Management Server

ESD
Electrostatic Discharge

ESP
Encapsulated Security Payload

F

FAZ
FortiAnalyzer

FCT
FortiClient

FDN
FortiGuard Distribution Network

FDS
FortiGuard Distribution Servers

FG
FortiGate

FGFM
FortiGate-FortiManager

FMG
FortiManager

FQDN
Fully Qualified Domain Name

FSA
FortiSandbox

FSSO
Fortinet Single Sign-On

FTP
File Transfer Protocol

G

GCF
Gatekeeper Confirm

GPRS
General Packet Radio Service

GRE
Generic Routing Encapsulation

GTP
GPRS Tunneling Protocol

GUI
Graphical User Interface

GUID
Globally Unique Identifier

H

HA
High Availability

hcache
Hard Cache

HDD
Hard Disk Drive

HTML
HyperText Markup Language

HTTP
HyperText Transfer Protocol

I

I/O
Input / Output

IBP
Identity-based Policy

ICAP
Internet Content Adaptation Protocol

ICMP
Internet Control Message Protocol

IGP
Interior Gateway Protocol

IKE
Internet Key Exchange

IMAP
Internet Message Access Protocol

IOC
Indicators of Compromise

IP
Internet Protocol

IPS
Intrusion Prevention System

IPsec
Internet Protocol Security

ISDB
Internet Service Database

ISP
Internet Service Provider

IV
Initialization Vector

J

JSON
JavaScript Object Notation

L

L2TP
Layer 2 Tunneling Protocol

LACP
Link Aggregation Control Protocol

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

M

MAC
Media Access Control

MD5
Message Digest 5

MGCP
Media Gateway Controller Protocol

MIB
Management Information Base

MMC
Microsoft Management Console

MSCHAP
Microsoft Challenge-Handshake Authentication Protocol

MSS
Maximum Segment Size

N

NAC
Network Access Control or Compliance

NAS
Network Access Server

NAT
Network Address Translation

NAT-PT
Network Address Translation (NAT) Port Translation

NDcPP
Network Device Collaborative Protection Profile

NGFW
Next-Generation Firewall

NNTP
Network News Transfer Protocol

NOC
Network Operations Center

NPU
Network Processing Unit

NTLM
NT LAN Manager

NTP
Network Time Protocol

O

OCSP
Online Certificate Status Protocol

OFTP
Odette File Transfer Protocol

ONC-RPC
Open Network Computing Remote Procedure Call

OSPF
Open Shortest Path First

OTP
One-time Password

OU
Organization Unit

OUI
Organizationally Unique Identifier

OVF
Open Virtualization Format

P

PAP
Password Authentication Protocol

PAT
Port Address Translation

PEM
Power Entry Module

PFS
Perfect Forward Secrecy

PKCS
Public Key Cryptography Standards

PKI
Public Key Infrastructure

PoE
Power over Ethernet

POP3
Post Office Protocol 3

PPP
Point-to-Point Protocol

PPPoE
Point-to-Point Protocol over Ethernet

PPTP
Point-to-Point Tunneling Protocol

PSK
Pre-Shared Key

R

RADIUS
Remote Authentication Dial-In User

RAID
Redundant Array of Independent Disks

RAM
Random Access Memory

RAS
Registration, Admission, and Status

RBAC
Role Based Access Control

RCF
Registration Confirm

RDP
Remote Desktop Protocol

REST
Representational State Transfer

RFC
Remote Function Call

RSH
Remote Shell

RSSO
RADIUS Single Sign-On

RTM
Real-Time Monitor

RTP
Real-Time Protection

RTSP
Real-Time Streaming Protocol

S

SAN
Storage Area Network

SAP
Shelf Alarm Panel

SCEP
Simple Certificate Enrollment Protocol

SCP
Secure Copy

SCVP
Server-based Certificate Validation Protocol

SDK
Software Development Kit

SDN
Software-Defined Networking

SFTP
Secure (or SSH) File Transfer Protocol

SHA1
Secure Hash Algorithm 1

SIP
Session Initiation Protocol

SMTP
Simple Mail Transfer Protocol

SNAT
Secure Network Address Translation

SNI
Server Name Indication

SNMP
Simple Network Management Protocol

SOC
Security Operations Center

SQL
Structured Query Language

SSH
Secure Shell

SSID
Service Set Identifier

SSL
Secure Sockets Layer

SSO
Single Sign-On

T

TACACS+
Terminal Access Controller Access-Control System

Tcl
Tool Command Language

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

TLS
Transport Layer Security

TNS
Transparent Network Substrate

TTL
Time-to-live

U

UDP
User Datagram Protocol

UID
Unique Identifier

URI
Uniform Resource Identifier

URL
Uniform Resource Locator

UTM
Unified Threat Management

UUID
Universally Unique Identifier

V

VDOM
Virtual Domain

VHD
Virtual Hard Disk

VIP
Virtual Internet Protocol

VLAN
Virtual Local Area Network

VM
Virtual Machine

VMDK
Virtual Machine Disk

VoIP
Voice over Internet Protocol

VPC
Virtual Private Cloud

VPN
Virtual Private Network

VSA
Vendor Specific Attribute

W

WAF
Web Application Firewall

WAN
Wide Area Network

WCCP
Web Cache Communication Protocol

WIDS
Wireless Intrusion Detection System

WPA
Wi-Fi Protected Access

WPA2
Wi-Fi Protected Access II

WSDL
Web Services Description Language

WTP
Wireless Transaction Protocol

X

XAuth
Extended Authentication

XML
eXtensible Markup Language

XSS
Cross-site Scripting

XVA
XenServer Virtual Appliance

Index

X